itprotect | scout

Функциональные характеристики

Для компании: АО «Инфозащита»

Дата: Москва, 2025 год

+7 (495) 786 34 93 | info@itprotect.ru | www.itprotect.ru

Содержание

1 Введение 6

1.1 Назначение документа 6

1.2 Область применения 6

1.3 Целевая аудитория 7

2 Функциональные характеристики 8

2.1 Глубокое профилирование внешней поверхности атаки с выявлением векторов проникновения 8

2.1.1 Режимы запуска сканирования 9

2.1.2 Процесс профилирования инфраструктуры 9

2.1.3 Формирование карты поверхности атаки 9

2.1.4 Выявление уязвимых компонентов и векторов атак 10

2.1.5 Представление результатов профилирования 11

2.2 Разведывательный анализ цифровых активов организации с картированием всех внешних точек входа 12

2.2.1 Ведение реестра цифровых активов 12

2.2.2 Управление и категоризация активов 13

2.2.3 Детальные карточки активов 13

2.2.4 Картирование точек входа 14

2.2.5 Интеграция с процессом сканирования 14

2.3 Детальное профилирование сетевых служб с определением версий ПО и конфигураций 15

2.3.1 Обнаружение и идентификация сетевых служб 15

2.3.2 Анализ конфигураций и настроек безопасности 16

2.3.3 Технологический стек и взаимосвязи 16

2.3.4 Мониторинг состояния служб 16

2.3.5 Интеграция с оценкой рисков 17

2.4 Корреляция обнаруженных уязвимостей с известными эксплойтами и техниками атак 17

2.4.1 Идентификация уязвимостей через стандартизированные базы 18

2.4.2 Анализ техник атак 18

2.4.3 Определение критичности в контексте инфраструктуры 19

2.5 Поиск цифровых следов организации в специализированных источниках киберразведки 19

2.5.1 Проверка учётных данных по базам утечек 19

2.5.2 Представление результатов поиска 20

2.6 Оперативное обнаружение модификаций в инфраструктуре для выявления подозрительной активности 20

2.6.1 Отслеживание изменений между сканированиями 20

2.6.2 Временные метрики изменений 21

2.6.3 Индикация подозрительной активности 21

2.7 Технические отчёты для служб безопасности с детализированными данными 22

2.7.1 Формирование отчётов в формате PDF 22

2.7.2 Управление отчётами 22

2.8 Детализированная оценка критичности угроз на основе вероятности эксплуатации 23

2.8.1 Интегральная оценка уровня угроз 23

2.8.2 Индивидуальная оценка каждой угрозы 23

2.8.3 Распределение угроз по категориям критичности 24

2.9 Экспертные рекомендации по реагированию на сложные векторы атак 24

2.9.1 Рекомендации в карточках проблем 24

2.9.2 Техническая детализация рекомендаций 25

2.10 Углублённый анализ нестандартных угроз силами экспертов 25

2.10.1 Опциональная услуга консультаций 25

2.11 Расширенные настройки для профессиональных пользователей 26

2.11.1 Управление профилем и безопасностью 26

2.11.2 Двухфакторная аутентификация 26

2.11.3 Управление сессиями 27

2.12 Защищённый веб-доступ с расширенными настройками безопасности для работы с конфиденциальными данными 27

2.12.1 Веб-интерфейс системы 27

2.12.2 Механизмы защиты доступа 27

3 Системные требования 28

3.1 Требования к серверной части 28

3.2 Требования к клиентской части 28

3.2.1 Минимальные аппаратные требования 28

3.2.2 Минимальные программные требования 29

3.2.3 Сетевые требования 30

4 Входные и выходные данные 30

4.1 Типы входных данных 30

4.1.1 Доменные имена 30

4.1.2 IP-адреса 31

4.1.3 Ограничения и валидация 31

4.2 Форматы выходных данных 31

4.2.1 Технические отчёты 31

4.2.2 Веб-интерфейс 32

4.2.3 Структурированные данные 32

4.3 Интеграционные возможности 33

4.3.1 Веб-доступ 33

4.3.2 Экспорт данных 33

1 Введение

1.1 Назначение документа

Настоящий документ содержит описание функциональных характеристик программного обеспечения ITProtect Scout (далее — ITProtect Scout, Система), предназначенного для углублённой разведки киберугроз и оперативного анализа индикаторов компрометации в корпоративной инфраструктуре организаций.

Документ определяет состав функций системы, входные и выходные данные, условия выполнения функций и ожидаемые результаты согласно принятым требованиям к оформлению программной документации.

1.2 Область применения

ITProtect Scout представляет собой специализированную систему кибербразведки, ориентированную на профессиональное использование службами информационной безопасности организаций, внешними аудиторами и консультантами по кибербезопасности.

Система предназначена для решения следующих задач:

- глубокое профилирование внешней поверхности атаки с выявлением векторов проникновения;
- разведывательный анализ цифровых активов организации с картированием всех внешних точек входа;
- детальное профилирование сетевых служб с определением версий программного обеспечения и конфигураций;
- корреляция обнаруженных уязвимостей с известными эксплойтами и техниками атак;

- поиск цифровых следов организации в специализированных источниках киберразведки;
- оперативное обнаружение модификаций в инфраструктуре для выявления подозрительной активности;
- формирование технических отчётов для служб безопасности с детализированными данными.

1.3 Целевая аудитория

Основными пользователями ITProtect Scout являются:

Службы информационной безопасности организаций:

- Специалисты SOC (Security Operations Center);
- Аналитики по информационной безопасности;
- Администраторы безопасности корпоративных систем;
- Руководители подразделений ИБ.

Внешние аудиторы и консультанты:

- Специалисты по проведению аудита информационной безопасности;
- Консультанты по кибербезопасности;
- Эксперты по анализу защищённости;
- Специалисты по пентестингу и этичному хакингу.

Специализированные организации:

- Центры мониторинга информационной безопасности;
- Компании-интеграторы решений ИБ;
- Поставщики управляемых услуг безопасности (MSSP);

- Организации, проводящие расследования инцидентов безопасности.

2 Функциональные характеристики

Программное обеспечение ITProtect Scout реализует комплекс функций для углублённой разведки киберугроз и оперативного анализа индикаторов компрометации в корпоративной инфраструктуре. Система обеспечивает полный цикл работы с внешним периметром организации: обнаружение и инвентаризацию активов, глубокий анализ уязвимостей, непрерывный мониторинг изменений и формирование технической отчётности.

Все функциональные возможности доступны через защищённый веб-интерфейс без необходимости установки локальных компонентов. Система работает в режиме SaaS (Software as a Service) и обеспечивает централизованное управление процессами сканирования и анализа результатов.

Далее представлено детальное описание реализованных функциональных возможностей в соответствии с требованиями технического задания.

2.1 Глубокое профилирование внешней поверхности атаки с выявлением векторов проникновения

В соответствии с требованиями к комплексному исследованию внешнего периметра организации, в системе ITProtect Scout реализованы следующие функциональные возможности:

2.1.1 Режимы запуска сканирования

Система поддерживает два режима инициирования процесса профилирования:

- Ручной запуск сканирования выполняется оператором через веб-интерфейс. Администратор выбирает необходимый пресет сканирования, определяющий параметры и глубину анализа, после чего инициирует проверку активов проекта.
- Автоматическое сканирование по расписанию настраивается администратором для каждого проекта. Система позволяет добавить проект в расписание сканирований с заданной периодичностью выполнения проверок.

2.1.2 Процесс профилирования инфраструктуры

При выполнении сканирования система осуществляет комплексный анализ внешнего периметра организации.

Идентификация активов производится для всех подтверждённых доменов и IP-адресов организации. Каждый актив проходит проверку доступности, определение открытых портов и запущенных служб. Система фиксирует тип актива, его текущий статус и время обнаружения.

Анализ сетевых служб включает определение запущенных сервисов на открытых портах, извлечение баннеров и отпечатков служб, идентификацию используемых протоколов. Для каждой обнаруженной службы фиксируется порт, протокол (TCP/UDP) и дополнительная техническая информация.

2.1.3 Формирование карты поверхности атаки

По результатам сканирования система формирует комплексное представление внешней инфраструктуры организации.

Реестр активов представляет собой структурированный список всех цифровых активов организации. Каждый актив отображается с указанием уровня риска через цветовую индикацию: (критический — красный, высокий — оранжевый, средний — жёлтый).

Для каждого актива указывается количество связанных проблем безопасности, дата первичного обнаружения и дата последней проверки.

Детальные карточки активов предоставляют исчерпывающую информацию о каждой точке входа в инфраструктуру. Карточка содержит общую информацию об активе, DNS-записи для доменных имён, перечень всех связанных проблем безопасности и историю изменений. Интерфейс позволяет просматривать техническую информацию и отслеживать динамику изменений актива во времени.

2.1.4 Выявление уязвимых компонентов и векторов атак

Система автоматически анализирует собранную информацию для идентификации проблем безопасности и потенциальных векторов атак.

Обнаружение уязвимостей выполняется путём анализа версий программного обеспечения и конфигураций служб. Каждая выявленная уязвимость классифицируется по типу угрозы и получает числовую оценку риска. Система идентифицирует уязвимости через CVE-идентификаторы, определяет категорию проблемы и фиксирует технические параметры: затронутый IP-адрес, порт, протокол и службу.

Анализ векторов проникновения включает выявление всех потенциальных путей компрометации инфраструктуры. Система определяет реальные векторы атаки, где существуют подтверждённые уязвимости с доступными методами эксплуатации, и потенциальные векторы, представляющие

теоретическую угрозу. Для каждого вектора формируется описание возможного сценария атаки.

Детализация проблем безопасности реализована через систему карточек проблем, содержащих техническое описание, уровень риска, категорию, затронутые компоненты, рекомендации по устранению и временные метрики.

2.1.5 Представление результатов профилирования

Результаты глубокого профилирования представляются в различных форматах для обеспечения полноты анализа состояния безопасности.

Дашборд системы отображает консолидированную информацию о состоянии защищённости. Общая оценка угроз представлена по шкале от 0 до 10, где визуально отображается текущий уровень риска. Статистика проблем разделена по уровням критичности с цветовой индикацией. Отдельно выводится информация о скомпрометированных учётных данных и обнаруженных векторах атак с разделением на реальные и потенциальные угрозы.

Технические отчёты формируются в формате PDF и содержат полную информацию о результатах профилирования. Отчёты включают перечень всех обнаруженных активов, выявленные уязвимости с детальным описанием, анализ векторов атак и рекомендации по устранению проблем. Формат отчётов адаптирован для использования специалистами служб информационной безопасности.

2.2 Разведывательный анализ цифровых активов организации с картированием всех внешних точек входа

В соответствии с требованиями к ведению реестра цифровых активов и картированию инфраструктуры, в системе реализованы следующие функциональные возможности:

2.2.1 Ведение реестра цифровых активов

Система обеспечивает полнофункциональное управление реестром цифровых активов организации через специализированный раздел «Активы».

Добавление активов в систему осуществляется администратором проекта вручную. Поддерживается внесение доменных имён и IP-адресов, которые составляют внешний периметр организации. При создании пользователя администратором автоматически устанавливается лимит в 50 активов, который может быть изменён при необходимости.

Процесс подтверждения активов реализован для обеспечения контроля над областью сканирования. Все добавленные активы требуют подтверждения администратором перед включением в процесс сканирования. Это гарантирует, что проверке подвергаются только легитимные ресурсы организации.

Валидация активов выполняется системой автоматически при добавлении. Корректно введённые активы отображаются на вкладке «На проверку», где администратор может подтвердить их принадлежность организации. Система контролирует формат вводимых данных и предотвращает добавление некорректных записей.

2.2.2 Управление и категоризация активов

Реестр активов предоставляет расширенные возможности управления и анализа.

Статусы и состояния активов отображаются в едином интерфейсе с возможностью быстрой визуальной оценки. Каждый актив имеет индикацию уровня риска через цветовую схему (см. раздел 2.1.3). Система отображает количество связанных с активом проблем безопасности.

Фильтрация и поиск реализованы для эффективной работы с большими объёмами данных. Доступна фильтрация по типу актива (домен или IP-адрес), уровню риска, статусу, датам обнаружения. Поисковая система позволяет быстро находить конкретные активы по названию или части адреса.

Сортировка активов поддерживается по всем ключевым параметрам: названию актива, уровню риска, типу, дате последнего обнаружения, дате первичного обнаружения. Для доменов дополнительно доступна сортировка по DNS-записям. Направление сортировки изменяется нажатием на заголовок соответствующего столбца.

2.2.3 Детальные карточки активов

Для каждого актива в системе формируется подробная карточка с исчерпывающей информацией.

Общая информация об активе включает основные характеристики: тип актива, текущий статус, уровень риска, даты первого и последнего обнаружения. Отображается принадлежность к проекту и общая статистика по связанным проблемам.

DNS-информация для доменов представлена на отдельной вкладке карточки. Система отображает все DNS-записи домена, включая A, AAAA,

MX, TXT, NS и другие типы записей. Это позволяет получить полное представление о конфигурации DNS и выявить потенциальные проблемы настройки.

Связанные проблемы безопасности отображаются непосредственно в карточке актива. Каждая проблема представлена с указанием уровня риска, CVE-идентификатора (при наличии), категории угрозы. Из карточки актива можно перейти к детальному описанию любой связанной проблемы.

История изменений актива фиксирует все модификации, обнаруженные в процессе мониторинга. Система отслеживает изменения в DNS-записях, появление или исчезновение служб, изменение статуса доступности.

2.2.4 Картирование точек входа

Система выполняет комплексное картирование всех внешних точек входа в инфраструктуру организации.

Автоматическое обнаружение связей между активами реализовано на основе анализа DNS-записей, WHOIS-информации и сетевой топологии. Система выявляет взаимосвязи между доменами и IP-адресами, определяет принадлежность к единой инфраструктуре.

Визуализация инфраструктуры через интерфейс активов позволяет получить целостное представление о внешнем периметре. Группировка по уровню риска помогает приоритизировать работу с проблемными активами.

2.2.5 Интеграция с процессом сканирования

Реестр активов тесно интегрирован с подсистемой сканирования.

Автоматическое обновление информации происходит после каждого сканирования. Система обновляет статусы активов, уровни риска, списки

обнаруженных проблем. Новая информация немедленно отображается в реестре и карточках активов.

Обнаружение новых активов в процессе сканирования приводит к их добавлению в реестр с пометкой о необходимости подтверждения. Администратор получает уведомление о появлении новых объектов и может принять решение о их включении в периметр мониторинга.

2.3 Детальное профилирование сетевых служб с определением версий ПО и конфигураций

В соответствии с требованиями к исследованию сетевых служб и идентификации технологического стека, в системе реализованы следующие функциональные возможности:

2.3.1 Обнаружение и идентификация сетевых служб

Система выполняет комплексное исследование всех доступных сетевых служб на обнаруженных активах.

Сканирование портов и протоколов осуществляется для каждого подтверждённого актива. Система идентифицирует открытые TCP и UDP порты, определяет запущенные на них службы. Для каждого обнаруженного порта фиксируется номер порта, используемый протокол транспортного уровня, тип и название службы.

Идентификация программного обеспечения выполняется через анализ баннеров служб и специфических откликов. Система определяет типы сервисов, включая веб-серверы (Apache, Nginx, IIS), почтовые серверы, базы данных, службы удалённого доступа. Для каждой службы, где это технически возможно, определяется версия программного обеспечения.

2.3.2 Анализ конфигураций и настроек безопасности

Система проводит детальный анализ конфигурационных параметров обнаруженных служб.

Выявление небезопасных конфигураций включает обнаружение служб с настройками по умолчанию, использование устаревших или небезопасных протоколов, отсутствие необходимых механизмов защиты. Каждая выявленная проблема конфигурации классифицируется по уровню риска.

Анализ криптографических параметров выполняется для служб, использующих шифрование. Система проверяет поддерживаемые алгоритмы шифрования, выявляет использование слабых криптографических алгоритмов (например, «Weak Encryption Algorithm(s) Supported (SSH)» или «Weak MAC Algorithm(s) Supported (SSH)»). Данные проблемы отображаются в общем реестре с указанием уровня риска.

2.3.3 Технологический стек и взаимосвязи

Определение технологического стека происходит через комплексный анализ всех обнаруженных компонентов. Система идентифицирует используемые технологии веб-приложений, определяет категории служб (например, «Web application abuses» для веб-приложений), выявляет специфические технологии защиты, такие как Anti-Scanner Defenses.

Категоризация служб реализована через систему классификации проблем. Каждая обнаруженная служба и связанная с ней проблема относится к определённой категории, что позволяет быстро оценить профиль технологических рисков организации.

2.3.4 Мониторинг состояния служб

Система отслеживает изменения в составе и конфигурации сетевых служб.

Фиксация времени обнаружения каждой службы и связанной проблемы позволяет отслеживать динамику изменений. Для каждой проблемы указывается дата первого обнаружения, дата последнего подтверждения, время жизни проблемы.

Отслеживание изменений в конфигурации служб происходит при каждом сканировании. Система фиксирует появление новых служб, изменение версий программного обеспечения, модификацию конфигурационных параметров.

2.3.5 Интеграция с оценкой рисков

Результаты профилирования сетевых служб интегрируются в общую систему оценки рисков.

Результаты профилирования сетевых служб интегрируются в общую систему оценки рисков, описанную в разделе 2.8.

Приоритизация проблем основана на совокупной оценке риска службы и связанных уязвимостей. Службы классифицируются по уровню риска согласно общей системе цветовой индикации (см. раздел 2.1.3).

2.4 Корреляция обнаруженных уязвимостей с известными эксплойтами и техниками атак

В соответствии с требованиями к сопоставлению выявленных уязвимостей с базами данных известных эксплойтов, в системе реализованы следующие функциональные возможности:

2.4.1 Идентификация уязвимостей через стандартизированные базы

Система выполняет автоматическое сопоставление обнаруженных проблем безопасности с международными базами уязвимостей.

Использование CVE-идентификаторов обеспечивает однозначную идентификацию известных уязвимостей. Каждая обнаруженная уязвимость, присутствующая в базе CVE, маркируется соответствующим идентификатором (например, CVE-2010-4755, CVE-2021-41617, CVE-2021-27065). Система предоставляет ссылки на базы CVE/NVD для получения детальной информации об эксплойтах и методах атаки.

Оценка применимости эксплойтов выполняется для каждой идентифицированной CVE-уязвимости. Система определяет, существуют ли публично доступные эксплойты для конкретной версии программного обеспечения и конфигурации службы.

2.4.2 Анализ техник атак

Категоризация по типам атак позволяет оценить характер угроз. Уязвимости классифицируются по категориям возможных атак, например «Web application abuses» для атак на веб-приложения, что помогает понять потенциальные векторы компрометации.

Оценка сложности эксплуатации отражается в числовой оценке риска. Уязвимости с простыми методами эксплуатации получают более высокую оценку риска, учитывая вероятность их использования злоумышленниками.

2.4.3 Определение критичности в контексте инфраструктуры

Расчёт уровня риска выполняется с учётом базовой оценки CVE и контекста инфраструктуры согласно методологии, описанной в разделе 2.8.

Приоритизация по вероятности эксплуатации обеспечивает фокус на наиболее опасных уязвимостях. Проблемы с известными эксплойтами и простыми методами атаки получают повышенный приоритет и выделяются соответствующей цветовой индикацией (см. раздел 2.1.3).

2.5 Поиск цифровых следов организации в специализированных источниках киберразведки

В соответствии с требованиями к проверке корпоративных email-адресов и мониторингу утечек данных, в системе реализованы следующие функциональные возможности:

2.5.1 Проверка учётных данных по базам утечек

Система осуществляет автоматическую проверку корпоративных email-адресов организации на предмет компрометации.

Мониторинг утечек паролей выполняется путём сопоставления email-адресов сотрудников с публичными базами скомпрометированных учётных данных. Система проверяет наличие корпоративных адресов в известных утечках и определяет статус каждой учётной записи.

Классификация учётных данных разделяет все проверенные записи на три категории:

- Скомпрометированные — учётные данные, обнаруженные в базах утечек;
- Рисковые — учётные записи с признаками потенциальной угрозы;
- Безопасные — учётные данные без признаков компрометации.

2.5.2 Представление результатов поиска

Статистика на дашборде отображает общее состояние учётных данных организации. Визуализация показывает количество записей в каждой категории, позволяя быстро оценить масштаб потенциальной компрометации.

Интеграция с общей оценкой угроз учитывает обнаруженные утечки при расчёте интегрального показателя безопасности. Наличие скомпрометированных учётных данных повышает общий уровень риска организации.

2.6 Оперативное обнаружение модификаций в инфраструктуре для выявления подозрительной активности

В соответствии с требованиями к выявлению изменений в инфраструктуре и идентификации признаков компрометации, в системе реализованы следующие функциональные возможности:

2.6.1 Отслеживание изменений между сканированиями

Система выполняет сравнительный анализ результатов последовательных сканирований для выявления изменений в инфраструктуре.

Фиксация новых объектов происходит при обнаружении ранее отсутствовавших элементов инфраструктуры. Система идентифицирует появление новых активов, открытие ранее закрытых портов, запуск новых служб. Все новые объекты требуют подтверждения администратором для включения в периметр мониторинга.

Мониторинг исчезновения элементов отслеживает прекращение доступности ранее обнаруженных компонентов. Система фиксирует закрытие портов, остановку служб, недоступность активов.

2.6.2 Временные метрики изменений

Фиксация временных характеристик обеспечивает понимание динамики изменений. Для каждого элемента инфраструктуры система сохраняет:

- Дату первого обнаружения объекта;
- Дату последнего подтверждения наличия;
- Время жизни проблемы или актива.

Классификация изменений по критичности выполняется автоматически на основе характера модификаций. Появление новых критических уязвимостей или высокорисковых служб получает повышенный приоритет и отражается в общей оценке угроз.

2.6.3 Индикация подозрительной активности

Выделение аномальных изменений происходит через систему цветовой индикации и уровней риска. Изменения, потенциально указывающие на компрометацию или подготовку к атаке, выделяются соответствующим уровнем угрозы.

Обновление статусов после сканирования обеспечивает актуализацию данных в системе. После завершения каждого сканирования все изменения отражаются в дашборде, реестре активов и связанных карточках.

2.7 Технические отчёты для служб безопасности с детализированными данными

В соответствии с требованиями к формированию подробных технических отчётов для специалистов ИБ, в системе реализованы следующие функциональные возможности:

2.7.1 Формирование отчётов в формате PDF

Система обеспечивает генерацию технических отчётов через специализированный раздел «Отчёты».

Создание отчётов выполняется на основе актуальных данных о состоянии инфраструктуры. Система формирует документ, содержащий результаты последнего сканирования, перечень обнаруженных проблем и рекомендации по устранению.

Скачивание документов реализовано в формате PDF, что обеспечивает универсальность использования и сохранение форматирования. Отчёты доступны для загрузки непосредственно из веб-интерфейса системы.

2.7.2 Управление отчётами

Раздел «Отчёты» предоставляет централизованный доступ к сформированным документам. Интерфейс позволяет просматривать список доступных отчётов, выполнять их скачивание для дальнейшего использования.

Пагинация и настройка отображения обеспечивают удобную работу с большим количеством отчётов. Система поддерживает настройку количества отображаемых записей и навигацию по страницам.

2.8 Детализированная оценка критичности угроз на основе вероятности эксплуатации

В соответствии с требованиями к расчёту критичности угроз с учётом вероятности их эксплуатации, в системе реализованы следующие функциональные возможности:

2.8.1 Интегральная оценка уровня угроз

Общий показатель безопасности рассчитывается системой автоматически и отображается на дашборде по шкале от 0 до 10. Визуальное представление оценки позволяет мгновенно определить текущий уровень защищённости инфраструктуры, где 0 соответствует отсутствию угроз, а 10 — критическому уровню опасности.

Алгоритм расчёта учитывает совокупность всех обнаруженных проблем, их уровни критичности и количество затронутых активов. Критические уязвимости вносят больший вклад в итоговую оценку, чем проблемы среднего или низкого уровня.

2.8.2 Индивидуальная оценка каждой угрозы

Числовая оценка риска присваивается каждой обнаруженной проблеме индивидуально. Значения варьируются в зависимости от характеристик угрозы (например, «3.4» для проблем среднего уровня, «10.0» для критических уязвимостей).

Факторы оценки включают техническую сложность эксплуатации, доступность уязвимого компонента из интернета, потенциальное воздействие на инфраструктуру. Система учитывает контекст конкретной инфраструктуры при определении итогового уровня риска.

2.8.3 Распределение угроз по категориям критичности

Группировка по уровням опасности представлена на дашборде в виде счётчиков:

- Критические угрозы (красная индикация)
- Высокие угрозы (оранжевая индикация)
- Средние угрозы (жёлтая индикация)

Такое распределение позволяет быстро оценить профиль рисков и приоритизировать работу по устранению проблем.

2.9 Экспертные рекомендации по реагированию на сложные векторы атак

В соответствии с требованиями к предоставлению рекомендаций по устранению угроз, в системе реализованы следующие функциональные возможности:

2.9.1 Рекомендации в карточках проблем

Текстовые описания проблем содержатся в каждой карточке обнаруженной уязвимости. Система предоставляет техническое описание сути проблемы, объясняющее характер угрозы и потенциальные последствия её эксплуатации.

Решения по устранению включены в карточку каждой проблемы в специальном поле "Решение". Рекомендации содержат конкретные шаги по нейтрализации угрозы, адаптированные для технических специалистов служб информационной безопасности.

2.9.2 Техническая детализация рекомендаций

Привязка к конкретным компонентам обеспечивает точность рекомендаций. Каждое решение учитывает специфику затронутого актива, службы, порта и протокола, что позволяет применять рекомендации без дополнительной адаптации.

2.10 Углублённый анализ нестандартных угроз силами экспертов

В соответствии с требованиями к поддержке экспертного анализа сложных угроз, в системе предусмотрены следующие возможности:

2.10.1 Опциональная услуга консультаций

Экспертная поддержка доступна как дополнительная услуга для проведения углублённого анализа нестандартных и сложных угроз. Услуга предоставляет возможность взаимодействия с экспертами по кибербезопасности для детального разбора результатов сканирования.

Область применения консультаций включает анализ нестандартных векторов атак, не покрываемых автоматическим сканированием, помощь в интерпретации сложных результатов, разработку индивидуальных стратегий реагирования на специфические угрозы.

2.11 Расширенные настройки для профессиональных пользователей

В соответствии с требованиями к реализации расширенных возможностей настройки для профессиональных пользователей, в системе реализованы следующие функциональные возможности:

2.11.1 Управление профилем и безопасностью

Раздел настроек предоставляет централизованный доступ к управлению параметрами учётной записи через вкладки: Профиль, Безопасность, Подписка, Уведомления, Интеграции.

Настройки безопасности включают:

- Изменение пароля учётной записи
- Настройку двухфакторной аутентификации (2FA)
- Управление активными сессиями с возможностью их завершения

2.11.2 Двухфакторная аутентификация

Активация 2FA выполняется через приложение-аутентификатор на мобильном устройстве. Система генерирует QR-код для связывания учётной записи с приложением. После сканирования кода пользователь вводит 6-значный код из приложения для подтверждения привязки.

Процесс аутентификации после активации 2FA требует ввода дополнительного кода при каждом входе в систему. При включении двухфакторной аутентификации система отправляет уведомление на почту пользователя.

Отключение 2FA доступно в настройках безопасности. Для отключения необходимо ввести актуальный код из приложения-аутентификатора.

2.11.3 Управление сессиями

Контроль активных сессий отображает все открытые подключения к учётной записи с информацией о времени и месте входа. Пользователь может завершить любую подозрительную сессию, обеспечивая дополнительный уровень контроля доступа.

2.12 Защищённый веб-доступ с расширенными настройками безопасности для работы с конфиденциальными данными

В соответствии с требованиями к обеспечению безопасного доступа к системе без установки локальных компонентов, реализованы следующие функциональные возможности:

2.12.1 Веб-интерфейс системы

Доступ через браузер обеспечивает работу с системой без необходимости установки дополнительного программного обеспечения. Система функционирует в режиме SaaS (Software as a Service) и доступна через защищенное соединение.

Поддержка современных браузеров гарантирует совместимость с актуальными версиями Chrome/Chromium, Safari, Firefox, Microsoft Edge. Интерфейс адаптирован для корректного отображения во всех поддерживаемых браузерах.

2.12.2 Механизмы защиты доступа

Защищенное соединение реализовано через использование протокола HTTPS для всех взаимодействий с системой. Это обеспечивает шифрование

передаваемых данных между браузером пользователя и серверами системы.

Контроль доступа к данным обеспечивается через систему авторизации с уникальными учётными записями для каждого пользователя. Разграничение прав доступа гарантирует, что пользователи имеют доступ только к данным своей организации.

3 Системные требования

3.1 Требования к серверной части

Поскольку ITProtect Scout функционирует в режиме SaaS, серверная инфраструктура полностью обеспечивается правообладателем. Система развёрнута в облачной инфраструктуре и не требует установки серверных компонентов на стороне пользователя.

3.2 Требования к клиентской части

3.2.1 Минимальные аппаратные требования

Компонент	Требования
Процессор	64-разрядный процессор с тактовой частотой 2,1 ГГц или выше, количество ядер — 2 или более
Оперативная память	4 ГБ или более

Компонент	Требования
Свободное дисковое пространство	10 ГБ или более
Разрешение экрана	1280×1024 пикселей или выше
Сетевой адаптер	Ethernet-адаптер с поддержкой скорости 100 Мбит/с или выше

3.2.2 Минимальные программные требования

Компонент	Требования
Операционная система	Windows 10 (версия 1909 или новее), Windows 11 macOS 10.14 (Mojave) или новее Linux (Ubuntu 20.04 LTS или новее, RHEL 8 или новее)
Веб-браузер	Google Chrome версии 90 или новее Mozilla Firefox версии 88 или новее Microsoft Edge версии 90 или новее Safari версии 14 или новее Opera версии 76 или новее

3.2.3 Сетевые требования

Параметр	Требования
Скорость подключения к сети Интернет	100 Мбит/с или выше
Протоколы	HTTPS (TLS 1.2 или выше)
Порты	TCP 443 (HTTPS)
Стабильность соединения	Постоянное подключение к сети Интернет

4 Входные и выходные данные

4.1 Типы входных данных

Система ITProtect Scout принимает и обрабатывает следующие типы входных данных для анализа внешней инфраструктуры организации:

4.1.1 Доменные имена

Система поддерживает добавление доменных имён различных уровней для включения в периметр сканирования. Поддерживаются домены второго и последующих уровней. Для каждого домена система автоматически выполняет:

- Валидацию корректности формата доменного имени;
- Разрешение DNS-записей;
- Определение связанных IP-адресов;

- Выявление поддоменов.

4.1.2 IP-адреса

Система принимает как отдельные IP-адреса, так и диапазоны адресов для сканирования:

- IPv4-адреса в стандартном формате;
- IPv6-адреса;
- Валидация корректности формата IP-адресов при вводе.

4.1.3 Ограничения и валидация

При добавлении активов в систему действуют следующие правила:

- Установлен базовый лимит в 50 активов на проект (может быть изменён администратором);
- Все активы проходят процедуру валидации формата при добавлении;
- Требуется подтверждение администратором перед включением в сканирование;
- Некорректные записи автоматически отклоняются системой.

4.2 Форматы выходных данных

4.2.1 Технические отчёты

Основным форматом экспорта результатов анализа являются технические отчёты в формате PDF, которые формируются системой на основе актуальных данных о состоянии инфраструктуры. Отчёты содержат результаты последнего выполненного сканирования, включая полный

перечень обнаруженных проблем безопасности с их детальным описанием и экспертными рекомендациями по устранению выявленных уязвимостей.

Доступ к сформированным отчётам осуществляется через специализированный раздел «Отчёты» веб-интерфейса системы, откуда документы могут быть загружены для дальнейшего использования. Формат PDF обеспечивает универсальность использования и сохранение форматирования при передаче между различными системами. Отчёты предназначены для документирования текущего состояния безопасности инфраструктуры и адаптированы для использования специалистами служб информационной безопасности.

4.2.2 Веб-интерфейс

Интерактивное представление данных через веб-интерфейс включает:

- Дашборд с визуализацией общей оценки угроз (0—10) и статистикой по уровням критичности;
- Таблицы активов с возможностью фильтрации, сортировки и пагинации;
- Карточки активов с детальной информацией, DNS-записями, связанными проблемами;
- Карточки проблем с техническим описанием, CVE-идентификаторами, рекомендациями;
- Визуальные индикаторы уровней риска через цветовую схему.

4.2.3 Структурированные данные

Система обеспечивает представление данных в структурированном виде:

- Перечень активов с атрибутами (тип, риск, статус, проблемы);

- Список проблем с техническими параметрами (CVE, CVSS, категория, порт, протокол);
- Временные метрики (даты обнаружения, время жизни проблем);
- Статистика по категориям угроз и векторам атак.

4.3 Интеграционные возможности

4.3.1 Веб-доступ

Система функционирует в режиме SaaS и предоставляет:

- Защищённый доступ через HTTPS-протокол;
- Поддержку современных браузеров (Chrome/Chromium, Safari, Firefox, Microsoft Edge);
- Работу без установки локальных компонентов;
- Централизованное управление через веб-интерфейс.

4.3.2 Экспорт данных

На текущий момент реализованы следующие возможности экспорта:

- Скачивание PDF-отчётов для дальнейшего использования;
- Возможность копирования данных из интерфейса для использования в других системах.